

# MINIMUM DISTANCE OF LINEAR CODES AND THE $\alpha$ -INVARIANT

MEHDI GARROUSIAN AND ȘTEFAN O. TOHĂNEANU

**ABSTRACT.** The simple interpretation of the minimum distance of a linear code obtained by De Boer and Pellikaan, and later refined by the second author, is further developed through the study of various finitely generated graded modules. We use the methods of commutative/homological algebra to find connections between the minimum distance and the  $\alpha$ -invariant of such modules.

## 1. INTRODUCTION

Let  $\mathcal{C}$  be an  $[n, k, d]$ -linear code with generating matrix (in canonical bases)

$$G = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix},$$

where  $a_{ij} \in \mathbb{K}$ , any field.

By this, one understands that  $\mathcal{C}$  is the image of the injective linear map

$$\phi : \mathbb{K}^k \xrightarrow{G} \mathbb{K}^n.$$

$n$  is the *length* of  $\mathcal{C}$ ,  $k$  is the *dimension* of  $\mathcal{C}$  and  $d$  is the *minimum distance* (or *Hamming distance*), the smallest number of non-zero entries in a non-zero codeword (i.e. non-zero element of  $\mathcal{C}$ ).

Also, for any vector  $w \in \mathbb{K}^n$ , the *weight* of  $w$ , denoted  $wt(w)$ , is the number of non-zero entries in  $w$ . A vector has at most  $m$  non-zero entries if and only if all products of  $m + 1$  distinct entries are zero. This simple observation was first exploited in the context of coding theory by De Boer and Pellikaan [2], in the following way:

Let  $\Sigma_{\mathcal{C}} = (\ell_1, \dots, \ell_n)$  denote the collection of linear forms in  $R := \mathbb{K}[x_1, \dots, x_k]$  dual to the columns of  $G$ , considered possibly with repetitions. Let  $I(\mathcal{C}, a) \subset R$  be the ideal generated by all  $a$ -fold products of the linear forms in  $\Sigma_{\mathcal{C}}$ , i.e.

$$I(\mathcal{C}, a) = \langle \{\ell_{i_1} \cdots \ell_{i_a} \mid 1 \leq i_1 < \cdots < i_a \leq n\} \rangle.$$

Then, by [2, Exercise 3.25], the minimum distance satisfies

$$d = \max\{a \mid ht(I(\mathcal{C}, a)) = k\}.$$

This result was refined in [16, Theorem 3.1] in the following way:  $\mathcal{C}$  has minimum distance  $d$  if and only if  $d$  is the maximal integer such that for any  $1 \leq a \leq d$ , one has  $I(\mathcal{C}, a) = \mathfrak{m}^a$ , where  $\mathfrak{m} = \langle x_1, \dots, x_k \rangle$ .

The above result was one of the initial motivations to study the connections between the minimum distance and some invariants coming from commutative/homological algebra. Commutative algebraic techniques have been used extensively in the study of evaluation codes, starting with the work of Hansen [9], yet to our knowledge, the interpretation of minimum distance as a homological invariant started showing up

---

2010 *Mathematics Subject Classification.* Primary 68W30; Secondary: 16W70, 52C35, 11T71.

*Key words and phrases.* minimum distance, Fitting ideal, filtration, inverse systems, Orlik-Terao algebra.

Garrousian's Address: Departamento de Matemáticas, Universidad de los Andes, Cra 1 No. 18A-12, Bogotá, Colombia, Email: m.garrousian@uniandes.edu.co

Tohaneanu's Address: Department of Mathematics, University of Idaho, Moscow, Idaho 83844-1103, USA, Email: tohaneanu@uidaho.edu, Phone: 208-885-6234, Fax: 208-885-5843.

with the famous Cayley-Bacharach theorem and its coding interpretation [8], and subsequently, [15], [17], and ultimately in [18]. In all these papers, the focus is to get bounds on the minimum distance from the minimal graded free resolution of the ideal of points corresponding to the columns of some generating matrix. The minimum socle degree of this ideal gives a lower bound for the minimum distance; so a half-satisfactory connection (since one does not obtain a formula). The most general result in this direction is [18, Theorem 2.8], that presents a lower bound on the minimum distance in terms of the  $\alpha$ -invariant of the defining ideal of a zero-dimensional fat points scheme.

The  $\alpha$ -invariant of a finitely generated graded module  $M = \bigoplus_{i \geq 0} M_i$ , denoted  $\alpha(M)$ , is the smallest  $i$  for which  $M_i \neq 0$ ; in other words, it is the smallest degree of a generator of  $M$ . Sometimes, this is called the  $a$ -invariant.

The ideals generated by  $a$ -fold products of linear forms do not form a filtration, though [16, Theorem 3.1] suggests that they are very close to the  $m$ -adic filtration. Because of this, in Section 2 we resort to a somewhat artificial construction that leads to a certain graded module whose  $\alpha$ -invariant we calculate. It turns out that this module is the Fitting module of a very simple graded module, and we obtain one of the main results in Theorem 2.1. In Section 2, we also find connections (see Theorem 2.2) with a vector space originally considered in [13], and explored further in [1]. In particular, [1] gives a short exact sequence of these vector spaces under the matroid operations of deletion and restriction. We obtain a similar sequence of Fitting modules for MDS codes (Theorem 2.5).

In Section 3 at the beginning we relate the minimum distance with the  $\alpha$ -invariant of Macaulay inverse systems ideal of the Chow form of a code; the lower bound we find is not very powerful, as it only attains equality in very few examples. This impels us to ask if it is possible to classify all  $\mathcal{C}$  for which this bound becomes equality. In the next part we work over  $\mathbb{F}_2$ ; this allows us to obtain a filtration out of the ideals generated by  $a$ -fold products of linear forms, and then find a formula for the minimum distance in terms of the  $\alpha$ -invariant of the positive degree part of an associated graded algebra corresponding to this filtration (see Theorem 3.7). In the last subsection we investigate connections with the Orlik-Terao algebra of an arrangement (associated to a linear code  $\mathcal{C}$ ): for codes of dimension 3 we discover an interesting lower bound for the minimum distance in terms of the length of the linear strand of the Orlik-Terao ideal. We end with a result (Proposition 2.5) showing that the minimal graded free resolution of the Orlik-Terao algebra is not enough to give complete information about the minimum distance of the code.

There are several ways to compute the minimum distance. One method (from [2]) is to iteratively calculate heights of ideals generated by  $a$ -fold products of linear forms, or calculate Gröbner bases of such ideals until one obtains a nonempty variety.

Another method comes from linear algebra: the minimum distance of an  $[n, k, d]$ -linear code with generating matrix  $G$ , is the number  $d$  such that  $n - d$  is the maximum number of columns of  $G$  that span a  $k - 1$  dimensional vector (sub)space (see for example, [18, Remark 2.2]). This second method gives also the geometrical interpretation of minimum distance: assuming that  $G$  has no proportional columns, then these columns are  $n$  distinct points in  $\mathbb{P}^{k-1}$ . Then  $n - d$  is the maximum number of these points that fit in a hyperplane.

The generating matrix  $G$  of a  $[n, k, d]$ -linear code  $\mathcal{C}$  naturally determines a matroid  $M(\mathcal{C})$ . The above linear algebraic interpretation suggests that the minimum distance is an invariant of the underlying matroid. This led us to an interesting observation on how to read off the minimum distance by looking at the Tutte polynomial of  $M(\mathcal{C})$ . By definition, the *Tutte polynomial* of  $M(\mathcal{C})$  (or just  $\mathcal{C}$ ) is

$$T_{\mathcal{C}}(x, y) = \sum_{I \subseteq [n]} (x - 1)^{k - r(I)} (y - 1)^{|I| - r(I)},$$

where  $r(I)$  is the dimension of the linear span of the columns of  $G$  indexed by  $I$ , and  $|I|$  is the cardinality of  $I$ .

There is a strong connection between this polynomial and the invariants of a code, especially the weight-enumerator polynomial; see [11] for a detailed review. The following lemma is included despite the fact that its proof is immediate since we are not aware of this formulation in the literature.

**Lemma 1.1.** *The minimum distance is determined by the largest power of  $y$  in a term of the form  $xy^p$  that appears in  $T_C(x+1, y)$ .*

$$d = n - p - k + 1.$$

*Also the coefficient of this term gives the number of projective codewords of minimum weight.*

We are not primarily concerned with developing new computational methods for finding the minimum distance. Our goal is rather to establish connections between the minimum distance with various classical homological invariants. Most of the proofs of our results are not very challenging; we believe that the merit of the notes lies within the interpretations of the minimum distance that we present in the statements of our results. For the background on linear codes we recommend the introductory pages of [11], and for commutative algebra (including a friendly introduction to filtrations) we suggest [4].

## 2. THE FITTING MODULE OF A LINEAR CODE

We begin with a classical construction in commutative algebra, see [5, Chapter A2G]. Let  $M$  be a finitely generated module over a ring  $R$ . Suppose  $M$  has a free presentation

$$R^m \xrightarrow{\phi} R^n \rightarrow M \rightarrow 0.$$

For  $1 \leq j \leq \min\{m, n\}$ , let  $I_j(\phi)$  denote the ideal of  $R$  generated by the  $j \times j$  minors of some matrix representation of  $\phi$ . By convention,  $I_j(\phi) = R$  if  $j \leq 0$ , and  $I_j(\phi) = 0$ , if  $j > \min\{m, n\}$ . Then the  $k$ -th Fitting ideal of  $M$  is the ideal

$$\text{Fitt}_j(M) := I_{n-j}(\phi).$$

The Fitting module of  $M$  is defined to be the  $R$ -module

$$\text{Fitt}(M) = \bigoplus_{j=0}^n \frac{\text{Fitt}_{n-j}(M)}{\text{Fitt}_{n-j-1}(M)}.$$

We are interested in the following situation:  $R = \mathbb{K}[x_1, \dots, x_k]$ ,  $\Sigma_C = (\ell_1, \dots, \ell_n)$  is the collection of linear forms in  $R$  we have seen in the introduction and  $M = \text{coker}(\phi) = \frac{R}{\langle \ell_1 \rangle} \oplus \dots \oplus \frac{R}{\langle \ell_n \rangle}$ , where

$$\phi = \text{diag}(\Sigma_C) = \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_n \end{bmatrix}.$$

One should observe the similarities with [5, Example A2.56].

For this setup, we denote  $\text{Fitt}(M)$  by  $\text{Fitt}(C)$ , and call this the Fitting module of the linear code  $C$ .

**Theorem 2.1.** *Let  $C$  be an  $[n, k, d]$ -linear code. Let  $\Sigma_C$  be the collection of  $n$  linear forms in  $R = \mathbb{K}[x_1, \dots, x_k]$  dual to the columns of some generating  $k \times n$  matrix of  $C$ . If  $\mathfrak{m} = \langle x_1, \dots, x_k \rangle$ , then the minimum distance of  $C$  satisfies*

$$d = \alpha(\mathfrak{m}\text{Fitt}(C)) - 1.$$

*Proof.* We have  $\phi = \text{diag}(\Sigma_C)$  and  $M = \text{coker}(\phi)$ . Then

$$\text{Fitt}_{n-j}(M) = I_j(\phi) = I(C, j),$$

which is the ideal generated by  $j$ -fold products we have seen in the introduction.

This is a homogeneous ideal generated in degree  $j$ . Also it is clear that  $I(\mathcal{C}, j+1) \subset I(\mathcal{C}, j)$ , for  $j = 1, \dots, n-1$ . Then

$$\text{Fitt}(\mathcal{C}) = \frac{R}{I(\mathcal{C}, 1)} \oplus \frac{I(\mathcal{C}, 1)}{I(\mathcal{C}, 2)} \oplus \dots \oplus \frac{I(\mathcal{C}, d-1)}{I(\mathcal{C}, d)} \oplus \frac{I(\mathcal{C}, d)}{I(\mathcal{C}, d+1)} \oplus \dots \oplus \frac{I(\mathcal{C}, n-1)}{I(\mathcal{C}, n)} \oplus I(\mathcal{C}, n).$$

As mentioned in the introduction,  $I(\mathcal{C}, j) = \mathfrak{m}^j$ ,  $j = 1, \dots, d$ . See [16, Theorem 3.1]. So

$$\mathfrak{m} \cdot \text{Fitt}(\mathcal{C}) = 0 \oplus \dots \oplus 0 \oplus \frac{\mathfrak{m}^{d+1}}{I(\mathcal{C}, d+1)} \oplus \dots \oplus \frac{\mathfrak{m} \cdot I(\mathcal{C}, n-1)}{I(\mathcal{C}, n)} \oplus \mathfrak{m}I(\mathcal{C}, n),$$

since  $I(\mathcal{C}, j+1) \subset \mathfrak{m} \cdot I(\mathcal{C}, j)$ , for all  $j \geq 0$ .

In the proof of [16, Proposition 2.4] there exists  $f \in R_d \setminus I(\mathcal{C}, d+1)$ , with  $\mathfrak{m} \cdot f \in I(\mathcal{C}, d+1)$ . This  $f$  is in fact an element of degree  $d$  in the saturation with respect to  $\mathfrak{m}$  of  $I(\mathcal{C}, d+1)$ . Avoiding such elements, let  $g \in R_d \setminus \text{sat}(I(\mathcal{C}, d+1))$ . Such an element exists since by [16, Lemma 2.2] this saturated ideal is intersection of codimension  $k-1$  prime ideals, and therefore itself has codimension  $k-1$ ; or by using [16, Lemma 2.1] and the fact that an ideal and its saturation have the same codimension. But if  $\mathfrak{m} \cdot g \in I(\mathcal{C}, d+1)$ , then  $g \in \text{sat}(I(\mathcal{C}, d+1))$ , contradiction. So

$$\alpha\left(\frac{\mathfrak{m}^{d+1}}{I(\mathcal{C}, d+1)}\right) = d+1.$$

If  $M_i, i = 1, \dots, n$  are some graded  $R$ -modules, then  $N := \oplus M_i$  becomes a graded  $R$ -module with the natural grading  $N_k = \{(m_1, \dots, m_n) | m_i \in (M_i)_k \text{ for all } 1 \leq i \leq n\}$ . Therefore  $\text{Fitt}(\mathcal{C})$ , and hence  $\mathfrak{m} \cdot \text{Fitt}(\mathcal{C})$  become graded  $R$ -modules (the latter being a submodule of the former). Therefore  $\alpha(\mathfrak{m}\text{Fitt}(\mathcal{C})) = d+1$ .  $\square$

In [1] an interesting vector space is presented; we will adjust everything to our notation. Let  $\mathcal{C}$  be an  $[n, k, d]$ -linear code with  $\Sigma_{\mathcal{C}} = (\ell_1, \dots, \ell_n) \subset R := \mathbb{K}[x_1, \dots, x_k]$ .

For any  $I \subset [n]$ , denote  $\ell_I = \prod_{i \in I} \ell_i$ , with the convention that  $\ell_{\emptyset} = 1$ . Let  $P(\mathcal{C})$  be the  $\mathbb{K}$ -vector subspace of  $R$  spanned by  $\ell_I$ , for all  $I \subset [n]$ . Then one has a decomposition:

$$P(\mathcal{C}) = \bigoplus_{0 \leq u \leq v \leq n} P(\mathcal{C})_{u,v},$$

where

$$P(\mathcal{C})_{u,v} = \text{Span}_{\mathbb{K}}\{\ell_I | \dim_{\mathbb{K}}(\text{Span}_{\mathbb{K}}\{\ell_j, j \in [n] - I\}) = u \text{ and } v = n - |I|\}.$$

We have  $0 \leq u \leq k$  since  $\text{Span}_{\mathbb{K}}\{\ell_j, j \in [n] - I\}$  is a subspace of  $\mathbb{K}^k$ .

Using  $P(\mathcal{C})$ , [1, Theorem 1.1] shows that the Tutte polynomial satisfies:

$$T_{\mathcal{C}}(x, y) = \sum_{0 \leq u \leq v \leq n} (x-1)^{k-u} y^{v-u} \dim_{\mathbb{K}} P(\mathcal{C})_{u,v}.$$

The connection between  $P(\mathcal{C})$  and  $\text{Fitt}(\mathcal{C})$  is the following:

**Theorem 2.2.** *There is an isomorphism of  $\mathbb{K}$ -vector spaces:*

$$P(\mathcal{C}) \simeq \text{Fitt}(\mathcal{C}) \otimes_R \mathbb{K}.$$

*Proof.* One has  $\text{Fitt}(\mathcal{C}) \otimes_R \mathbb{K} = \frac{\text{Fitt}(\mathcal{C})}{\mathfrak{m}\text{Fitt}(\mathcal{C})}$ . The later  $\mathbb{K}$ -vector space is isomorphic to

$$\frac{R}{\mathfrak{m}} \oplus \frac{\mathfrak{m}}{\mathfrak{m}^2} \oplus \dots \oplus \frac{\mathfrak{m}^d}{\mathfrak{m}^{d+1}} \oplus \frac{I(\mathcal{C}, d+1)}{\mathfrak{m}I(\mathcal{C}, d+1)} \oplus \dots \oplus \frac{I(\mathcal{C}, n-1)}{\mathfrak{m}I(\mathcal{C}, n-1)} \oplus \frac{I(\mathcal{C}, n)}{\mathfrak{m}I(\mathcal{C}, n)}.$$

For all  $j = 1, \dots, n$ ,

$$\frac{I(\mathcal{C}, j)}{\mathfrak{m}I(\mathcal{C}, j)} = I(\mathcal{C}, j)_j = \text{Span}_{\mathbb{K}}\{\ell_{i_1} \dots \ell_{i_j} | 1 \leq i_1 < \dots < i_j \leq n\}.$$

With  $I(\mathcal{C}, 0)_0 = R_0 = \mathbb{K}$ , the isomorphism is clear.  $\square$

**Remark 2.3.**

- If  $|I| = n - v$ , then  $|\{j; j \in [n] - I\}| = v$ , and therefore  $\dim_{\mathbb{K}}(\text{Span}_{\mathbb{K}}\{\ell_j, j \in [n] - I\}) \leq v$ . This leads to  $\bigoplus_{0 \leq u \leq v} P(\mathcal{C})_{u,v} = I(\mathcal{C}, n - v)_{n-v}$ , for all  $v = 0, \dots, n$ .
- In the spirit of Lemma 1.1, if  $p = n - d - k + 1$ , then the coefficient of  $xy^p$  in  $T_{\mathcal{C}}(x + 1, y)$  is  $\dim_{\mathbb{K}} P(\mathcal{C})_{k-1, n-d}$ . The following is an explanation as to why this dimension equals the number of projective codewords of minimum weight.

From [16], projective codewords of minimum weight are in one-to-one correspondence with the points of the zero-dimensional variety  $V(I(\mathcal{C}, d + 1)) \subset \mathbb{P}^{k-1}$ . All the associated primes of the defining ideal of this variety are prime ideals of codimension  $k - 1$ , generated (not minimally) by  $n - d$  linear forms. So if  $P \in V(I(\mathcal{C}, d + 1))$  with ideal  $I_P = \langle \ell_{i_{d+1}}, \dots, \ell_{i_n} \rangle$ , then none of the complementary linear forms  $\ell_{i_1}, \dots, \ell_{i_d}$  vanishes at  $P$ . Denote  $J(P) = \{i_1, \dots, i_d\}$ .

Suppose one has  $P_1, \dots, P_s$  such points, with  $\ell_{J(P_1)}(P_1), \dots, \ell_{J(P_s)}(P_s) \neq 0$ , and suppose

$$c_1 \ell_{J(P_1)} + \dots + c_s \ell_{J(P_s)} = 0,$$

for some  $c_i \in \mathbb{K}$ . Evaluating this at  $P_i$ , since  $\ell_{J(P_j)}(P_i) = 0, i \neq j$ , one has that  $c_i = 0$ , giving that  $\ell_{J(P_1)}, \dots, \ell_{J(P_s)}$  are linearly independent.

- The coding theoretical equivalent of [1, Theorem 5.1] is [16, Theorem 3.1].

**2.1. Deletion-restriction.** Let  $\mathcal{C}$  be an  $[n, k, d]$ -linear code with generating matrix  $G$ . The *puncturing* of  $\mathcal{C}$  at the  $i$ -th column of  $G$  is the linear code denoted  $\mathcal{C} \setminus i$  with generating matrix obtained from  $G$  by removing the  $i$ -th column. If the dimension of  $\mathcal{C} \setminus i$  is  $k - 1$ , then  $d = 1$ , which is a very particular situation (in this case  $i$  is called a *coloop*). So, if  $i$  is not a coloop, then the parameters of  $\mathcal{C} \setminus i$  are  $[n - 1, k, d(i)]$ , where the minimum distance  $d(i)$  equals  $d$  or  $d - 1$ .

We are interested in puncturing  $\mathcal{C}$  at a column  $i$  of  $G$  that has the last entry  $\neq 0$ . Doing row operations on  $G$  one can assume that this column is of the form  $\begin{bmatrix} 0 & \dots & 0 & 1 \end{bmatrix}^T$ .

Let  $\mathcal{C}/i$  be the *shortening* of  $\mathcal{C}$  at the above  $i$ -th column of  $G$ . This is a linear code with generating matrix  $G_i$  obtained from  $G$ , by deleting the last row and this  $i$ -th column. Geometrically we restrict the hyperplanes  $V(\ell_i)$  to the hyperplane  $V(x_k)$ . The linear code  $\mathcal{C}/i$  has parameters  $[n - 1, k - 1, d_i]$ . In general,  $d_i \geq d(i)$ .

From now on, let us assume  $i = n$ , and we denote  $\mathcal{C} \setminus n$  and  $d(n)$  by  $\mathcal{C}'$  and  $d'$ , respectively; and we denote  $\mathcal{C}/n$  and  $d_n$  by  $\mathcal{C}''$  and  $d''$ , respectively.

At the level of Fitting ideals one can immediately show that

$$I(\mathcal{C}, a) = x_k I(\mathcal{C}', a - 1) + I(\mathcal{C}', a), a = 1, \dots, n \quad (2.1.1)$$

and

$$I(\mathcal{C}, a) + \langle x_k \rangle = I(\mathcal{C}', a) + \langle x_k \rangle = I(\mathcal{C}'', a) + \langle x_k \rangle. \quad (2.1.2)$$

In matroidal terms, “puncturing” and “shortening” of  $\mathcal{C}$  correspond to “deletion” and “restriction (contraction)” of  $M(\mathcal{C})$ .

**2.1.1. MDS codes.** [1, Lemma 6.2] shows that the vector space  $P(\mathcal{C})$  behaves very well under deletion and restriction, whereas our Fitting modules behave in a more complicated manner. However, if  $\mathcal{C}$  is an MDS code (i.e.,  $d = n - k + 1$ ), we can obtain a similar short exact sequence of  $R := \mathbb{K}[x_1, \dots, x_k]$ -modules. Here, we have  $R'' := \mathbb{K}[x_1, \dots, x_{k-1}] = R/\langle x_k \rangle$ , which gives the Fitting module of the restriction a natural  $R$ -module structure.

It is not difficult to see that if  $\mathcal{C}$  is an MDS code, then  $\mathcal{C}'$  and  $\mathcal{C}''$  are also MDS codes. Combinatorially,  $\mathcal{C}$  is MDS if and only if the underlying matroid  $M(\mathcal{C})$  is isomorphic to the uniform matroid  $U_{k,n}$  (see [11, page 49]).

In order to obtain our result, we have to look at *star configurations* in  $\mathbb{P}^{k-1}$  (see [7] for relevant details). For  $1 \leq c \leq k-1$ , consider the ideal  $I_{V_c}$  of the star configuration  $V_c$ :

$$V_c = \bigcup_{1 \leq i_1 < \dots < i_c \leq n} H_{i_1} \cap \dots \cap H_{i_c}, \quad I_{V_c} = \bigcap_{1 \leq i_1 < \dots < i_c \leq n} \langle \ell_{i_1}, \dots, \ell_{i_c} \rangle.$$

**Lemma 2.4.** ([7, Proposition 2.9]) *Let  $\mathcal{C}$  be an MDS code with parameters  $[n, k, n-k+1]$ . Then, for  $d+1 = n-k+2 \leq j \leq n$ ,*

- (1)  $I(\mathcal{C}, j) = I_{V_{n-j+1}}$  and
- (2) if  $c = n-j+1$ , the Hilbert series satisfies

$$HS(R/I_{V_c}, t) = \frac{\sum_{u=0}^{n-c} \binom{c-1+u}{c-1} t^u}{(1-t)^{k-c}}.$$

*Proof.* From the beginning of Section 2 in [16], it follows that  $I(\mathcal{C}, j) \subseteq I_{V_{n-j+1}}$ .

The proof of [7, Proposition 2.9(4)] makes use of the equation 2.1.1, to show by induction that  $I_{V_{n-j+1}} \subseteq I(\mathcal{C}, j)$ .

The second part is immediate from [7].  $\square$

**Theorem 2.5.** *Let  $\mathcal{C}$  be an  $[n, k]$  MDS code, and let  $\ell \in \Sigma_{\mathcal{C}}$ . Let  $\mathcal{C}'$  and  $\mathcal{C}''$  be the deletion and restriction at  $\ell$ , respectively. Then one has a short exact sequence of  $R$ -modules*

$$0 \longrightarrow \text{Fitt}(\mathcal{C}')(-1) \xrightarrow{\cdot \ell} \text{Fitt}(\mathcal{C}) \longrightarrow \text{Fitt}(\mathcal{C}'') \longrightarrow 0.$$

*Proof.* Assume  $\ell = x_k$ , and denote  $I_a := I(\mathcal{C}, a) \subset R$ ,  $I'_a := I(\mathcal{C}', a) \subset R$  and  $I''_a := I(\mathcal{C}'', a) \subset R''$ . As we have discussed earlier,  $\mathcal{C}$  is an  $[n, k, d]$ -linear code,  $\mathcal{C}'$  is an  $[n-1, k, d-1]$ -linear code, and  $\mathcal{C}''$  is an  $[n-1, k-1, d]$ -linear code with  $d = n-k+1$ .

Equations 2.1.1 and 2.1.2 give rise to the following short exact sequence of  $R$ -modules, determined by multiplication by  $x_k$ :

$$0 \longrightarrow \frac{R}{I_{a+1} : x_k}(-1) \longrightarrow \frac{R}{I_{a+1}} \longrightarrow \frac{R}{I_{a+1} + \langle x_k \rangle} \simeq \frac{R''}{I''_{a+1}} \longrightarrow 0,$$

for all  $a = 0, \dots, n$ .

For  $a+1 \geq d+1$ , computing the Hilbert series of the first term via the short exact sequence above, using Lemma 2.4 (with  $c = c' = n-a$  and  $c'' = n-a-1$ ), one has

$$\begin{aligned} t \cdot HS(R/(I_{a+1} : \langle \ell \rangle), t) &= HS(R/I_{a+1}, t) - HS(R''/I''_{a+1}, t) \\ &= \frac{\sum_{u=0}^a \left( \binom{n-a-1+u}{n-a-1} - \binom{n-a-2+u}{n-a-2} \right) t^u}{(1-t)^{k-a-1}} \\ &= \frac{\sum_{u=1}^a \binom{n-a-2+u}{n-a-1} t^u}{(1-t)^{k-a-1}} \\ &= \frac{t \sum_{u=0}^{a-1} \binom{n-a-1+u}{n-a-1} t^u}{(1-t)^{k-a-1}} = t \cdot HS(R/I'_a, t). \end{aligned}$$

Since  $I'_a \subseteq I_{a+1} : x_k$ , from above we get in fact the equality  $I'_a = I_{a+1} : x_k$ .

If  $a < d$ , then, by [16, Theorem 3.1],  $I_{a+1} = \langle x_1, \dots, x_k \rangle^{a+1}$ ,  $I_a = \langle x_1, \dots, x_k \rangle^a$ , and  $I''_{a+1} = \langle x_1, \dots, x_{k-1} \rangle^{a+1}$ .

Since  $\langle x_1, \dots, x_k \rangle^{a+1} : x_k = \langle x_1, \dots, x_k \rangle^a$  and  $\langle x_1, \dots, x_k \rangle^{a+1} + \langle x_k \rangle = \langle x_1, \dots, x_{k-1} \rangle^{a+1} + \langle x_k \rangle$ , for all  $a = 0, \dots, n$  we have the short exact sequence of  $R$ -modules:

$$0 \longrightarrow \frac{R}{I'_a}(-1) \longrightarrow \frac{R}{I_{a+1}} \longrightarrow \frac{R''}{I''_{a+1}} \longrightarrow 0.$$

Snake Lemma applied to the surjective map of complexes

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{R}{I'_{a-1}}(-1) & \longrightarrow & \frac{R}{I_a} & \longrightarrow & \frac{R''}{I''_a} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \frac{R}{I'_a}(-1) & \longrightarrow & \frac{R}{I_{a+1}} & \longrightarrow & \frac{R''}{I''_{a+1}} \longrightarrow 0 \end{array}$$

leads to the short exact sequence of  $R$ -modules

$$0 \longrightarrow \frac{I'_{a-1}}{I'_a}(-1) \longrightarrow \frac{I_a}{I_{a+1}} \longrightarrow \frac{I''_a}{I''_{a+1}} \longrightarrow 0,$$

for all  $a = 0, \dots, n$ .

Taking the direct sum of all them, one obtains the claimed statement.  $\square$

### 3. OTHER CONNECTIONS AND RESULTS

**3.1. Inverse systems.** For this subsection the base field  $\mathbb{K}$  is a field of zero or sufficiently large characteristic.

Let  $\partial(V) := \mathbb{K}[\partial_1, \dots, \partial_k]$  where  $V = \mathbb{K}^k$  and  $\partial_i$  is a short hand notation for  $\partial/\partial_{x_k}$ .  $\partial(V)$  acts on  $R = \mathbb{K}[x_1, \dots, x_k]$  in the usual way where  $\partial_i(x_j) = \delta_{i,j}$ , extended by linearity and the Leibniz rule.

Let  $P \in R_r$ . Then the set  $\text{Ann}(P) := \{\theta \in \partial(V) | \theta P = 0\}$  is a homogeneous ideal of  $\partial(V)$ ; furthermore  $\partial(V)/\text{Ann}(P)$  is Artinian Gorenstein. As consequences of this result (also known as ‘‘Macaulay’s Inverse Systems Theorem’’) one has

- (1) The Castelnuovo-Mumforde regularity  $\text{reg}(\partial(V)/\text{Ann}(P)) = \deg(P) = r$ .
- (2) The Hilbert function of  $\partial(V)/\text{Ann}(P)$  in degree  $i$  (i.e.,  $HF(\partial(V)/\text{Ann}(P), i) = \dim_{\mathbb{K}}(\partial(V)/\text{Ann}(P))_i$ ) equals the dimension of the vector space spanned by the partial derivatives of order  $i$  of  $P$ .
- (3) From the Gorenstein property one can obtain the symmetry of the Hilbert function of  $R/\text{Ann}(P)$ , i.e.,  $HF(\partial(V)/\text{Ann}(P), i) = HF(\partial(V)/\text{Ann}(P), r - i)$ , for all  $i = 0, \dots, r$ .

For details about inverse systems [6] is a good source.

Let  $\mathcal{C}$  be an  $[n, k, d]$ -linear code with  $\Sigma_{\mathcal{C}} = (\ell_1, \dots, \ell_n) \subset R$ . Let  $\text{cf}(\mathcal{C}) = \prod_{i=1}^n \ell_i$ , be the *Chow form* of  $\mathcal{C}$ . In the next result, we see again the  $\alpha$ -invariant showing up.

**Proposition 3.1.** *If  $\text{char}(\mathbb{K}) > n$ , or  $\text{char}(\mathbb{K}) = 0$ , then*

$$d \geq \alpha(\text{Ann}(\text{cf}(\mathcal{C}))) - 1.$$

*Proof.* Denote  $I := \text{Ann}(\text{cf}(\mathcal{C}))$  and  $\alpha := \alpha(I)$ .

For all  $j = 0, \dots, \alpha - 1$ , one has

$$HF(\partial(V)/I, j) = \binom{k-1+j}{k-1}.$$

From the symmetry of the Hilbert function of  $\partial(V)/I$ , we have that for all  $j = 0, \dots, \alpha - 1$

$$HF(\partial(V)/I, n-j) = \binom{k-1+j}{k-1},$$

and therefore, from item (2) above,

$$\dim_{\mathbb{K}} \text{Span}(D^{n-j}(\text{cf}(\mathcal{C}))) = \binom{k-1+j}{k-1}.$$

Since  $\text{cf}(\mathcal{C}) = \prod_{i=1}^n \ell_i$ , then

$$\text{Span}(D^{n-j}(\text{cf}(\mathcal{C}))) \subseteq \text{Span}(\{\ell_{i_1} \cdots \ell_{i_j}\}_{1 \leq i_1 < \dots < i_j \leq n}),$$

and therefore

$$HF(I(\mathcal{C}, j), j) = \binom{k-1+j}{k-1} = HF(\langle x_1, \dots, x_k \rangle^j, j).$$

Since  $I(\mathcal{C}, j)$  is generated by forms of degree  $j$ , we conclude that

$$I(\mathcal{C}, j) = \langle x_1, \dots, x_k \rangle^j,$$

for all  $0 \leq j \leq \alpha - 1$ . From [16, Theorem 3.1], one obtains  $d \geq \alpha - 1$ .  $\square$

**Remark 3.2.** One can prove Proposition 3.1 without the use of the commutative algebraic machinery. Consider  $\text{cf}(\mathcal{C})$  the Chow form of  $\mathcal{C}$ . A codeword of minimum weight of  $\mathcal{C}$  corresponds to a point through which  $m := n - d$  linear forms of  $\Sigma_{\mathcal{C}}$  will pass. Suppose this point is  $Q := [0, \dots, 0, 1] \in \mathbb{P}^{k-1}$ , and suppose  $\ell_1(Q) = \dots = \ell_m(Q) = 0$ , and hence  $\ell_1, \dots, \ell_m \in \mathbb{K}[x_1, \dots, x_{k-1}]$ . Then

$$\text{cf}(\mathcal{C}) = (\ell_1 \cdots \ell_m) \cdot (\ell_{m+1} \cdots \ell_n).$$

One has

$$\partial_k^{d+1}(\text{cf}(\mathcal{C})) = (\ell_1 \cdots \ell_m) \cdot \partial_k^{d+1}(\ell_{m+1} \cdots \ell_n).$$

The later equals 0, as  $\deg(\ell_{m+1} \cdots \ell_n) = d$ . So  $\partial_k^{d+1} \in \text{Ann}(\text{cf}(\mathcal{C}))$ .

**Example 3.3.** One question is to analyse the arrangements for which equality in Theorem 3.1 holds true. For some linear codes (even MDS codes) this happens, but for most of them it doesn't.

Consider  $\mathcal{C}_1$  defined by the generating matrix  $G_1$ . It has minimum distance  $d = 2 = 4 - 3 + 1$ , so it is an MDS code. Computations with [10] give that  $\alpha(\text{Ann}(xyz(x + y + z))) = 3 = d + 1$ .

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix}$$

Consider  $\mathcal{C}_2$  with generating matrix  $G_2$ . It has minimum distance  $d = 3 = 5 - 3 + 1$ , so it is an MDS code. Computations with [10] give that  $\alpha(\text{Ann}(xyz(x + y + z)(x + 2y + 5z))) = 3 < d + 1$ .

**3.2. The case of binary codes.** Let  $S := \mathbb{K}[y_1, \dots, y_n]$  and consider the ring epimorphism

$$\gamma : S \rightarrow R, \gamma(y_i) = \ell_i, 1 \leq i \leq n.$$

The kernel of  $\gamma$ , denoted here  $F(\mathcal{C})$ , is an ideal of  $S$ , minimally generated by  $n - k$  linear forms in  $S$ . This is often called the *relation space* of  $\Sigma_{\mathcal{C}}$ . The matrix of the coefficients of the standard basis of  $F(\mathcal{C})$  is a  $(n - k) \times n$  matrix which is the generating matrix of the dual code of  $\mathcal{C}$ . Standard refers to the fact that transpose of this matrix is the parity-check matrix of  $\mathcal{C}$ . If  $G = [I_k | P]$ , then  $G^\perp = [-P^T | I_{n-k}]$ .

It is well known that a vector  $\mathbf{w} = (w_1, \dots, w_n)$  is in  $\mathcal{C}$ , if and only if the point  $(w_1, \dots, w_n)$  belongs to the linear variety with defining ideal  $F(\mathcal{C})$ . Also, a vector  $\mathbf{w} = (w_1, \dots, w_n)$  has weight  $\leq a - 1$ , if and only if all the distinct  $a$  products of its entries vanish. Equivalently, the point  $(w_1, \dots, w_n)$  is in the variety with defining ideal

$$I(Y, a) := \langle \{y_{i_1} \cdots y_{i_a} | 1 \leq i_1 < \dots < i_a \leq n\} \rangle,$$

which is the ideal of  $S$  generated by the  $a$ -fold products of  $Y := (y_1, \dots, y_n)$ .

With this, one obtains immediately that  $\mathcal{C}$  has minimum distance  $d$  if and only if it is the largest integer such that

$$\sqrt{F(\mathcal{C}) + I(Y, a)} = \langle y_1, \dots, y_n \rangle, \quad (3.2.1)$$

for all  $a = 1, \dots, d$ . It is clear from this that if one considers the linear code  $\mathcal{D}$  of length  $2n - k$  and dimension  $n$  with generating matrix  $[(G^\perp)^T | I_n]$ , and then shortens it to the first  $n - k$  columns, the new code has minimum distance  $d$  (in fact, this code is up to permutations and rescaling the same as  $\mathcal{C}$ ).



From now on our base field  $\mathbb{K}$  will be  $\mathbb{F}_2$ . Any element of  $\mathbb{F}_2$  satisfies the field equation  $X^2 = X$ , so we are going to consider the finite dimensional  $\mathbb{F}_2$ -algebra

$$\mathbb{S} := S / \langle y_1^2 - y_1, \dots, y_n^2 - y_n \rangle.$$

Let  $S \rightarrow \mathbb{S} : f \mapsto \bar{f}$  be the natural reduction map.

**Proposition 3.4.** *The linear code  $\mathcal{C}$  has minimum distance  $d$  if and only if in  $\mathbb{S}$  one has*

$$\bar{F}(\mathcal{C}) + \bar{I}(Y, a) = \langle \bar{y}_1, \dots, \bar{y}_n \rangle,$$

for all  $a = 1, \dots, d$ , where  $d$  is maximal with this property.

*Proof.* Formula 3.2.1 says that  $y_i^{n_i} \in F(\mathcal{C}) + I(Y, a)$ ,  $i = 1, \dots, n$ , for some  $n_i \geq 1$ . But in  $\mathbb{S}$ , we have  $\bar{y}_i^{n_i} = \bar{y}_i$ . Hence the result.  $\square$

**3.2.1. Standard filtration.** The algebra  $\mathbb{S}$  is a filtered algebra, with “standard” filtration given by the  $\mathbb{S}$ -modules:

$$\mathbb{S}_j := \mathbb{S} / \bar{I}(Y, j+1), j = 0, \dots, n.$$

Indeed one has

$$\mathbb{F}_2 = \mathbb{S}_0 \subset \mathbb{S}_1 \subset \dots \subset \mathbb{S}_n = \mathbb{S},$$

with  $\mathbb{S}_a \cdot \mathbb{S}_b \subseteq \mathbb{S}_{a+b}$ .

Proposition 3.4 immediately implies the following.

**Corollary 3.5.**  *$\mathcal{C}$  has minimum distance  $d$  if and only if  $d$  is the maximal integer such that for any  $a = 1, \dots, d$ , one has*

$$\frac{\mathbb{S}}{\bar{F}(\mathcal{C})} \otimes_{\mathbb{S}} \mathbb{S}_a = \mathbb{F}_2,$$

as  $\mathbb{S}$ -modules.

**3.2.2. Another filtration.** On  $\mathbb{S}$  there is also a filtration given by the ideals  $\bar{I}(Y, a)$ :

$$\mathcal{F}_\bullet : 0 \subset \underbrace{\bar{I}(Y, n)}_{\mathcal{F}_0} \subset \underbrace{\bar{I}(Y, n-1)}_{\mathcal{F}_1} \subset \dots \subset \underbrace{\bar{I}(Y, 1)}_{\mathcal{F}_{n-1}} \subset \underbrace{\bar{I}(Y, 0)}_{\mathcal{F}_n} = \mathbb{S}.$$

**Lemma 3.6.**  *$\mathcal{F}_\bullet$  is a filtration on  $\mathbb{S}$ , meaning that*

- (1)  $\mathbb{S} = \cup_i \mathcal{F}_i$ .
- (2)  $\mathcal{F}_a \cdot \mathcal{F}_b \subset \mathcal{F}_{a+b}$ .

*Proof.* The first statement is obvious.

For the second, let  $\bar{y}_{i_1} \dots \bar{y}_{i_{n-a}} \in \mathcal{F}_a$  and  $\bar{y}_{j_1} \dots \bar{y}_{j_{n-b}} \in \mathcal{F}_b$ . Suppose that  $|\{i_1, \dots, i_{n-a}\} \cap \{j_1, \dots, j_{n-b}\}| = c$ , with  $0 \leq c \leq \min\{n-a, n-b\}$ .

Since in  $\mathbb{S}$ , one has  $\bar{y}_u^2 = \bar{y}_u$ , for any  $u$ , one obtains

$$(\bar{y}_{i_1} \dots \bar{y}_{i_{n-a}}) \cdot (\bar{y}_{j_1} \dots \bar{y}_{j_{n-b}}) \in \bar{I}(Y, 2n-a-b-c).$$

Since  $2n-a-b-c \geq n-a-b$ , one has that

$$\bar{I}(Y, 2n-a-b-c) \subseteq \bar{I}(Y, n-a-b) = \mathcal{F}_{a+b}.$$

Hence the second statement is shown.  $\square$

On  $\mathbb{S} / \bar{F}(\mathcal{C})$  one has the induced filtration  $\mathcal{F}_\bullet(\mathbb{S} / \bar{F}(\mathcal{C})) = (\bar{F}(\mathcal{C}) + \mathcal{F}_\bullet) / \bar{F}(\mathcal{C})$ . So one can consider the associated graded module

$$\text{gr}_{\mathcal{F}_\bullet}(\mathbb{S} / \bar{F}(\mathcal{C})) := \bigoplus_{i=0}^n \frac{\mathcal{F}_i(\mathbb{S} / \bar{F}(\mathcal{C}))}{\mathcal{F}_{i-1}(\mathbb{S} / \bar{F}(\mathcal{C}))}.$$

The main result of this subsection is the following homological interpretation of the minimum distance, connecting once again to the  $\alpha$  invariant of graded modules.

**Theorem 3.7.** *With the above notations*

$$\alpha(\mathrm{gr}_{\mathcal{F}_\bullet}(\mathbb{S}/\bar{F}(\mathcal{C}))_+) = n - d.$$

*Proof.* The proof is immediate from observing that for all  $u = n - 1, \dots, n - d$

$$\mathcal{F}_u(\mathbb{S}/\bar{F}(\mathcal{C})) = \frac{\bar{F}(\mathcal{C}) + \bar{I}(\mathcal{Y}, n - u)}{\bar{F}(\mathcal{C})} = \frac{\langle \bar{y}_1, \dots, \bar{y}_n \rangle}{\bar{F}(\mathcal{C})},$$

the second equality being the result of Proposition 3.4.

Taking appropriate quotients, one obtains the result.  $\square$

**3.3. The Orlik-Terao algebra.** Let  $\mathbb{K}$  be any field, and let  $\mathcal{C}$  be an  $[n, k, d]$ -linear code with  $\Sigma_{\mathcal{C}} = (\ell_1, \dots, \ell_n) \subset R := \mathbb{K}[x_1, \dots, x_k], \gcd(\ell_i, \ell_j) = 1, i \neq j$ . Define a ring epimorphism

$$\phi : S := \mathbb{K}[y_1, \dots, y_n] \rightarrow \mathbb{K}[1/\ell_1, \dots, 1/\ell_n], \phi(y_i) = 1/\ell_i. \quad (3.3.1)$$

The Orlik-Terao algebra is  $\mathrm{OT}(\mathcal{C}) := \mathbb{K}[y_1, \dots, y_n]/\ker(\phi)$ .  $\ker(\phi)$  is called the Orlik-Terao ideal, and it is denoted  $\mathrm{IOT}(\mathcal{C})$ .

It is well known that  $\mathrm{IOT}(\mathcal{C})$  is generated by

$$\partial(a_1 y_{i_1} + \dots + a_u y_{i_u}) := \sum_{j=1}^u a_j y_{i_1} \cdots \widehat{y_{i_j}} \cdots y_{i_u}, \quad (3.3.2)$$

where  $a_1 y_{i_1} + \dots + a_u y_{i_u}, a_j \neq 0$  is an element in the relations space  $F(\mathcal{C})$  we have seen at the beginning of the previous subsection. Properties of  $\mathrm{OT}(\mathcal{C})$  can be found, for example in [3], and the citations therein.

**Remark 3.8.** Recall that  $\mathcal{C} = \mathrm{Im} G = \{\mathbf{x}G : \mathbf{x} \in \mathbb{K}^k\}$  and  $V(F(\mathcal{C})) = \ker G = \{\mathbf{y} \in \mathbb{K}^n : G\mathbf{y} = 0\}$  have dimensions  $k$  and  $n - k$ , respectively. As mentioned already,  $F(\mathcal{C}) = \mathcal{C}^\perp$ .

$$\begin{array}{ccc} \mathbb{K}^k & \xrightarrow{G} & \mathbb{K}^n \\ \downarrow \mathrm{id} & & \downarrow \mathrm{crem} \\ \mathbb{K}^k & \xrightarrow{\phi^*} & \mathbb{K}^n \end{array} \quad (3.3.3)$$

Let  $T = (\mathbb{K}^*)^\times$  be the  $n$ -dimensional torus. The vertical map is the Cremona transformation  $T \rightarrow T$ ,  $\mathbf{y} = (y_1, \dots, y_n) \mapsto \mathbf{y}^{-1} = (y_1^{-1}, \dots, y_n^{-1})$ . The linear space of the code  $\mathcal{C}$  is the vanishing of the maximal minors of the following augmented matrix.

$$\mathcal{C} = \{\mathbf{y} : \mathrm{rank} \begin{bmatrix} G & \\ y_1 & \cdots & y_n \end{bmatrix} = k\}$$

The variety defined by the OT is called the *reciprocal plane* which is the closure of the image of  $\mathcal{C} \cap T$  under the transformation. Alternatively, [3, Proposition 2.6] implies that the OT ideal can be obtained as the colon ideal  $\mathrm{IOT}(\mathcal{C}) = (I : y_1 \cdots y_n)$ , where  $I$  is generated by the maximal minors of the following matrix.

$$\begin{bmatrix} a_{11}y_1 & \cdots & a_{1n}y_n \\ \vdots & \ddots & \vdots \\ a_{k1}y_1 & \cdots & a_{kn}y_n \\ \hline 1 & \cdots & 1 \end{bmatrix}$$

The connection between the OT ideals of  $\mathcal{C}$  and  $\mathcal{C}^\perp$  is that they come from reciprocal planes of orthogonal spaces.

In order to calculate the minimum distance  $d$ , we are interested in codewords (so points in  $V(F(\mathcal{C}))$ ) with lots of zero entries,  $n - d$  to be precise. From the remarks above,  $\mathcal{C}$  and  $\mathrm{OT}(\mathcal{C})$  interact very well while inside the torus, hence to find points with zero coordinates one needs to investigate the fiber over zero of the

Orlik-Terao algebra, also called “the relative Orlik-Terao algebra” (see [3] for more details). It is still not clear how one can obtain a nice description of  $d$  from this approach; this path will be the focus of a future study.

**3.3.1. Length of linear strand.** Let  $M$  be a finitely generated graded  $S$ -module with  $\alpha(M) = \alpha$ . Suppose that the minimal graded free resolution of  $M$  has the shape

$$0 \rightarrow \mathbf{F}_n \rightarrow \cdots \rightarrow \mathbf{F}_{\delta+1} \rightarrow S^{n_\delta}(-(\alpha + \delta)) \oplus \mathbf{F}_\delta \rightarrow \cdots \rightarrow S^{n_0}(-\alpha) \oplus \mathbf{F}_0 \rightarrow M \rightarrow 0,$$

where  $\alpha(\mathbf{F}_j) \geq \alpha + j + 1$ , or they are zero. Then  $\delta$  is called *the length of the linear strand* of  $M$ .

From now on we will assume  $k = 3$ . So we are looking at  $\mathcal{C}$  with parameters  $[n, 3, d]$ .

**Proposition 3.9.** *Let  $\mathcal{C}$  be an  $[n, 3, d]$ -linear code with nonproportional linear forms of  $\Sigma_{\mathcal{C}}$ . Let  $\delta$  denote the length of the linear strand of the Orlik-Terao ideal  $\text{IOT}(\mathcal{C})$ , which is assumed not to be the zero ideal. Then*

- (1) *If  $\alpha(\text{IOT}(\mathcal{C})) = 3$ , then  $\mathcal{C}$  is an MDS code.*
- (2) *If  $\alpha(\text{IOT}(\mathcal{C})) = 2$ , then  $d \geq n - \delta - 3$ .*

*Proof.* If  $\alpha(\text{IOT}(\mathcal{C})) = 3$ , then any 3 of the linear forms in  $\Sigma_{\mathcal{C}}$  are linearly independent, hence the claim (1).

Suppose  $\alpha(\text{IOT}(\mathcal{C})) = 2$ . Denote  $\mathcal{A}$  to be the rank 3 arrangement of lines in  $\mathbb{P}^2$  with lines  $H_i = V(\ell_i)$ . Let  $X \in L_2(\mathcal{A})$ , and suppose  $X = H_1 \cap \cdots \cap H_p$ , with  $p \geq 3$ , maximal as possible (hence  $p = n - d$ ).

By [12, Theorem 3.1], the Orlik-Terao ideal of  $\mathcal{A}_X := \{H_1, \dots, H_p\}$  has linear graded free resolution of length  $p - 2$ . Since  $\text{IOT}(X) \subseteq \text{IOT}(\mathcal{C})$ , and the minimal generators of the former ideal (which are quadratic) are also part of the minimal generating set of the latter, one obtains

$$\delta \geq p - 3.$$

Since  $p = n - d$ , one obtains (2). □

At this moment we are not aware as to generalizing Proposition 3.9 to arbitrary  $k \geq 4$ . For example, [12, Theorem 3.4] says that the length of the linear strand of the Orlik-Terao ideal of a graphic arrangement is  $\leq 1$  all the time, regardless of  $k$ .

Equality in statement (2) is attained quite often. Two examples that violate this are the Braid arrangement and the non-Fano arrangement: in both cases  $n - d = 3$  and  $\delta = 1$ . This is due to the fact that the linear dependence among the relations give an unexpected linear syzygy (in a way, a converse of [12, Proposition 3.6]).

Suppose we have a relation on some 3-relations:

$$a_1 r_1 + \cdots + a_s r_s = 0, a_i \neq 0$$

and suppose the support of the relation  $r_l$  is  $\Lambda_l = \{i_l, j_l, k_l\}$ .

If  $i \in \Lambda_1$  but  $i \notin \cup_{j \neq 1} \Lambda_j$ , then since the term  $a_1 y_i$  must be zero, we get  $a_1 = 0$  which contradicts  $a_1 \neq 0$ . So

$$\forall l, \Lambda_l \subset \cup_{j \neq l} \Lambda_j,$$

or, in other words, every index occurs at least 2 times in two different supports of relations.

Assume  $\cup_{j=1}^s \Lambda_j = \{1, \dots, t\}$ .

Suppose we take the union of all supports  $\Lambda_i$  and account for the repeats. We are going to have  $3s$  indices. Each index is between  $\{1, \dots, t\}$  and it occurs at least twice. Therefore

$$3s \geq 2t.$$

This leads to the following lemma.

**Lemma 3.10.** *Let  $X_1, \dots, X_s \in L_2(\mathcal{A})$  and let  $r_i \in F(\mathcal{A}_{X_i}), i = 1, \dots, s$  be 3-relations with supports  $\Lambda_1, \dots, \Lambda_s$ , and with  $|\cup_i \Lambda_i| = t$ . If  $3s < 2t$ , then there is no linear syzygy on  $\partial(r_1), \dots, \partial(r_s)$ .*

Lemma 3.10 is saying that if one has few multiple points, then the length of the linear strand is determined solely by the maximum multiplicity of such a multiple point.

We end with a warning given by the following proposition, similar in flavor with [18, Example 4.1].

**Proposition 3.11.** *The minimum distance of a linear code  $\mathcal{C}$  is not determined solely by the graded betti numbers of the Orlik-Terao algebra of  $\mathcal{C}$ .*

*Proof.* The following have been computed with [10].

Consider the linear code  $\mathcal{C}_1$  with parameters  $[6, 3, 3]$  and  $\Sigma_{\mathcal{C}_1} = (x, y, z, x - y, x - z, y - z)$ . The minimal graded free resolution of  $\text{OT}(\mathcal{C}_1)$  is:

$$0 \longrightarrow S^2(-5) \longrightarrow S^3(-4) \oplus S^2(-3) \longrightarrow S^4(-2) \longrightarrow S \longrightarrow \text{OT}(\mathcal{C}_1).$$

Consider the linear code  $\mathcal{C}_2$  with parameters  $[6, 3, 2]$  and  $\Sigma_{\mathcal{C}_2} = (x, y, x + y, x - y, z, y - z)$ . The minimal graded free resolution of  $\text{OT}(\mathcal{C}_2)$  is:

$$0 \longrightarrow S^2(-5) \longrightarrow S^3(-4) \oplus S^2(-3) \longrightarrow S^4(-2) \longrightarrow S \longrightarrow \text{OT}(\mathcal{C}_2).$$

Same minimal graded free resolution, yet different minimum distances.  $\square$

**Acknowledgement** We thank Tristram Bogart for comments and corrections on improving the readability of our work.

## REFERENCES

- [1] A. Berget, *Products of linear forms and Tutte polynomials*, European J. Combin. **31**(2010), 1924–1935.
- [2] M. De Boer and R. Pellikaan, *Grobner Bases for Codes*, in Some Tapas of Computer Algebra, pp. 237–259, Springer, Berlin 1999.
- [3] G. Denham, M. Garrousian and S. Tohaneanu, *Modular decomposition of the Orlik-Terao algebra of a hyperplane arrangement*, Annals of Combinatorics **18**(2014), 289–312.
- [4] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.
- [5] D. Eisenbud, *The Geometry of Syzygies*, Springer-Verlag, New York 2005.
- [6] A.V. Geramita, *Inverse Systems of Fat Points: Waring’s Problem, Secant Varieties of Veronese Varieties, and Parameter Spaces for Gorenstein Ideals*, Queens Papers Pure Appl. Math. **102** (1996), 1–114.
- [7] A.V. Geramita, B. Harbourne and J. Migliore, *Star configurations in  $\mathbb{P}^n$* , J. Algebra **376** (2013), 279–299.
- [8] L. Gold, J. Little and H. Schenck, *Cayley-Bacharach and evaluation codes on complete intersections*, J. Pure Appl. Algebra **196** (2005), 91–99.
- [9] J. Hansen, *Points in uniform position and maximum distance separable codes*, in Zero-Dimensional Schemes (Ravello, 1992), de Gruyter, Berlin, 1994, pp. 205–211.
- [10] D. Grayson and M. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at <http://www.math.uiuc.edu/Macaulay2/>.
- [11] R. Jurrius and R. Pellikaan, *Codes, arrangements and matroids*, in Series on Coding Theory and Cryptology vol. 8, Algebraic Geometry Modeling in Information Theory, E. Martnez-Moro Ed., pp. 219–325, World Scientific 2013.
- [12] H. Schenck and S. Tohaneanu, *The Orlik-Terao algebra and 2-formality*, Math. Res. Lett. **16**(2009), 171–182.
- [13] P. Orlik and H. Terao, *Commutative algebras for arrangements*, Nagoya Math. J. **134** (1994), 65–73.
- [14] H. Terao, *Algebras generated by reciprocals of linear forms*, J. Algebra **250**(2002), 549–558.
- [15] S. Tohaneanu, *Lower bounds on minimal distance of evaluation codes*, Appl. Algebra Eng. Commun. Comput. **20** (2009), 351–360.
- [16] S. Tohaneanu, *On the De Boer-Pellikaan method for computing minimum distance*, J. Symbolic Comput. **45**(2010), 965–974.
- [17] S. Tohaneanu, *The minimum distance of sets of points and the minimum socle degree*, J. Pure Appl. Algebra **215** (2011), 2645–2651.
- [18] S. Tohaneanu and A. Van Tuyl, *Bounding invariants of fat points using a Coding Theory construction*, J. Pure Appl. Algebra **217**(2013), 269–279.